修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　　電気通信学研究科　　情報通信工学　専攻　博士前期課程		
氏　　名	王　磊	学籍番号	0730055
論 文 題 目	ハッシュ関数の安全性解析 Cryptanalysis of hash functions		

要　旨

最近，ハッシュ関数の安全性解析の研究が盛んである．MD4 や MD5 のような，広く使われているいくつかの Hash 関数は解読されている．暗号プロトコルが安全でない Hash 関数を利用するとき，そのプロトコルの安全が低下する可能性があるので，その安全性評価が重要となる．このことが，本研究の主たる動機である．本研究では，APOP(Authenticated Post Office Protocol) および HMAC/NMAC の安全性について議論する．

APOP は，チャレンジ-レスポンス型の認証プロトコルであり，メールシステムで使われている．この方式は，完全に破られており．既存の攻撃を無力化するために APOP の強化方法の候補がいくつか考えられる．本研究では，次の二つの強化案に焦点をあてて検討する．

候補１：チャレンジを ASCII コードに限定する対策

チャレンジを ASCII コードに限定したとしても攻撃が有効となるような，新しいメッセージ差分を提案する．その結果，パスワード回復攻撃は，依然として動作することとなる．

候補２：ユーザからの応答の計算方法を Hash(Password||Challenge)と変更する対策(従来は Hash(Challenge||Response)だった)：

MD4 についてパスワード回復方法を提案する．これは，実際に使われているわけではないので，理論的な研究である．研究の結果，2^{37} 回のオンライン状態での質問と 2^{21} 回分の MD4 の計算量で，パスワードの 16 文字を復元できることが明らかになった．

次に鍵つきハッシュに基づいたメッセージ認証コード HMAC/NMAC は，プロトコルや暗号システムで広く応用されている．本研究では，HMAC/NMAC-MD4 と NMAC-MD5 の鍵回復攻撃を提案する．従存の攻撃法に比べて、攻撃成功のために必要とする質回数、　計算量を削減できることが分かる。